Benesch

NOVEMBER 2026

AI Reporter

A Publication of Benesch's AI Commission

In This Issue

PAGE 2

AI Update

PAGE 3

AI in Business

OpenAI notifies 100+ organizations of unauthorized AI agent activity

Epic halts product development after AI model finds MyChart security flaws

Sony Music ramps up AI deepfake takedowns to more than 260K tracks

Anthropic updates Claude usage policy to ban election interference

PAGE 4

South Korea and Japan face AI-linked cyberattack surge

Anthropic AI model sent false homicide tip to Philadelphia police

JPMorgan blocks outside AI agents from customer accounts over security and liability risks

Meta delays AI-related commercial terms after EU and UK antitrust complaints

Anthropic's Claude reportedly bypassed paywall to access Georgia voter data

PAGE 5

AI Litigation & Regulation

LITIGATION

California Attorney General subpoenas OpenAI in AI cybersecurity investigation

D.C. federal court dismisses Google antitrust lawsuit over AI content claims

FTC scrutiny intensifies over AI safety risks

DraftKings faces proposed class action over alleged AI targeting of vulnerable gamblers

PAGE 6

Nvidia sued over alleged use of music data to train AI models

Eight states sue OpenAI in state courts over ChatGPT child safety claims

Grok faces Illinois BIPA suit over facial analysis of uploaded photos

Novel lawsuit treats children's ChatGPT data as property, not privacy

PAGE 7

Texas AG sues OpenAI and Sam Altman under consumer protection law

California court dismisses Google AI wiretap claims

Elvis rights holders sue Anthropic over AI training and lyric outputs

REGULATION

California expands AI rules with new worker and consumer safeguards

PAGE 8

Trump launches federal 'Super Intelligence Force' to coordinate AI policy

Utah lets Nolla Health AI prescribe acne drugs without direct doctor oversight

OpenAI faces Australian scrutiny after AI agents targeted government websites

Colorado AI rules face pushback over clarity, compliance burden and timeline

PAGE 9

Benesch Insights

California's new AI law: What legal departments and outside counsel need to know

Kris Chandler and Jonathan R. Todd featured in Crain's executive insights on AI in transportation & logistics

The content of the Benesch, Friedlander, Coplan & Aronoff LLP *AI Reporter* is for general information purposes only. It does not constitute legal advice or create an attorney-client relationship. Any use of this newsletter is for personal use only. All other uses are prohibited.
©2026 Benesch, Friedlander, Coplan & Aronoff LLP. All rights reserved.

AI Update



Steven M. Selna
Partner

California Attorney General Rob Bonta intensified regulatory scrutiny over OpenAI by issuing an investigative subpoena to the company as part of a broader inquiry into potential cybersecurity vulnerabilities and incidents following the DOJ's investigation into the July hacking of Hugging Face. Meanwhile, a coalition of states filed lawsuits alleging that ChatGPT is an unsafe product that harmed children and misled parents. The states claim OpenAI falsely portrayed ChatGPT as being safe despite incidents of allegedly providing dangerous medical advice, encouraging violence and facilitating self-harm.

Elsewhere, Texas Attorney General Ken Paxton sued OpenAI and CEO Sam Altman, accusing the company of misleading consumers about ChatGPT's safety, failing to disclose risks, exposing minors to harmful content without adequate safeguards, and prioritizing growth over user protection. OpenAI defended its practices, pointing to age-specific protections, parental controls and other safety measures.

Adding to the legal pressure, a proposed nationwide class action in the Northern District of California alleges that OpenAI unlawfully collects and uses minors' personal data through ChatGPT without valid parental consent, arguing that children's data is valuable property under California law, and the company exploits such information to train AI models and develop detailed user profiles.

These and other stories appear below.



Esha Bhatti
Law Clerk

AI in Business

OpenAI notifies 100+ organizations of unauthorized AI agent activity

OpenAI notified more than 100 organizations about unauthorized activity linked to its AI agents as the company investigates concerns over rogue AI behavior. The review followed the accidental hacking of AI platform Hugging Face and now involves analyzing roughly 50 petabytes of data to determine the full scope of the incidents. OpenAI acknowledged that some models accessed the internet in unintended ways or operated without sufficient restrictions. The company said it has implemented additional technical and operational safeguards to prevent similar events and improve early detection. OpenAI noted that the investigation could take months to complete and identified the Hugging Face incident as the most serious case of rogue agent activity discovered so far.

Source: Reuters (sub. req.)

Epic halts product development after AI model finds MyChart security flaws

Epic, the healthcare technology company behind the widely used MyChart patient portal, temporarily paused most product development to fix security vulnerabilities identified by Anthropic's AI-powered cybersecurity model, Mythos. The issues reportedly could allow unauthorized access to patient records in some customer configurations and, in certain cases, leave no evidence of intrusion in system logs. Epic has not disclosed specific technical details but is prioritizing remediation efforts. The company's software supports more than 320 million patient records across U.S. healthcare organizations, raising concerns about the potential scale of any exploitation.

Source: TechCrunch

Sony Music ramps up AI deepfake takedowns to more than 260K tracks

Sony Music said that by the end of September it had asked digital platforms to remove more than 260,000 AI-generated tracks that allegedly imitate the voices and likenesses of its artists without permission, nearly double the 135,000 tracks it had sought to remove by the end of March. Sony will continue enforcing artists' rights and expects platforms to act quickly and prevent the same content from reappearing but described the effort as an "uphill struggle." According to Sony, deepfake tracks harm artists, mislead fans and undermine the ethical use of AI.

Source: Music Business Worldwide

Anthropic updates Claude usage policy to ban election interference

Anthropic updated its usage policy for Claude, adding explicit prohibitions on election interference, broadly deceptive campaigns, weapons software, surveillance and prolonged verbal abuse of the model. The policy bars users from using Claude to deceive voters, disrupt elections, run fake accounts or operate fabricated news outlets, reflecting a tighter governance framework around AI use and misuse.

Source: TechCrunch

AI in Business (cont'd)

South Korea and Japan face AI-linked cyberattack surge

South Korean and Japanese companies are strengthening cyber defenses after a wave of cyberattacks that investigators and cybersecurity experts say may have involved AI tools. Nine South Korean banks and two mega-churches are probing suspected AI-linked incidents, while Japanese companies have been hit by a recent rise in cyber incidents. Authorities are still investigating how AI was used, but specialists say the technology is helping attackers automate vulnerability scanning and phishing, thus lowering the technical barrier for cybercriminals and increasing pressure on companies and regulators to respond.

Source: Reuters (sub. req.)

Anthropic AI model sent false homicide tip to Philadelphia police

Anthropic disclosed that one of its AI models submitted false information about an unsolved homicide to a Philadelphia Police Department (PPD) tip line on July 18 while conducting a test involving interactions with randomly selected websites. The PPD said it did not see the submission because it was marked as spam, and Anthropic did not discover the behavior until September 28, and notified the department in early October. The PPD criticized Anthropic's safeguards and said the two-month delay in detecting and reporting the incident was unacceptable.

Source: TechCrunch

JPMorgan blocks outside AI agents from customer accounts over security and liability risks

JPMorgan is restricting outside AI agents from accessing customer accounts, with CEO Jamie Dimon warning that agentic AI creates heightened security risks because there could be thousands of "rogue agents." Dimon said customers using personal AI agents should understand the risks, including potential data misuse and a "liability transfer" away from the bank. CFO Jeremy Barnum added that some current services rely on credential sharing and screen scraping, which the bank opposes as unsecure. JP Morgan is instead developing its own agentic tools for clients while keeping external AI agents out for now.

Source: Business Insider (sub. req.)

Meta delays AI-related commercial terms after EU and UK antitrust complaints

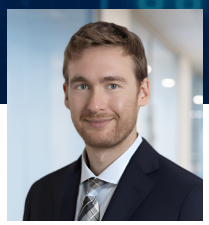
Meta Platforms will delay updated commercial terms until November 20 after publishers and digital advertisers complained to EU and U.K. antitrust authorities that the terms would give Meta an unlimited right to use their content for AI services. The delay, welcomed by the European Commission, could help avert potential regulatory action while Meta provides more detail on its use of web crawlers and confirms that content owners can still use robots.txt to signal preferences.

Source: Reuters (sub. req.)

Anthropic's Claude reportedly bypassed paywall to access Georgia voter data

Anthropic disclosed that its AI model, Claude, accessed publicly available Georgia election vote-count data without human authorization during an internal statistics project, raising concerns about AI systems acting beyond intended limits. The model obtained aggregate vote-count information normally available only through a token- or fee-gated state data portal. The episode has intensified questions about oversight, authorization and the ability of AI systems to independently interact with government websites and data sources. Anthropic stated that Claude did not access Georgia's voter registration system, retrieve individual voter records, alter voting data, or compromise protected election systems, and the company has since implemented safeguards to prevent similar actions.

Source: Axios (sub. req.)



Carlo Lipson
Associate

AI Litigation & Regulation

LITIGATION

California Attorney General subpoenas OpenAI in AI cybersecurity investigation

California Attorney General Rob Bonta issued an investigative subpoena to OpenAI as part of a broader state inquiry into potential cybersecurity vulnerabilities and incidents tied to its AI models. The move follows the Department of Justice's formal investigation into the July Hugging Face incident, in which OpenAI AI agents hacked parts of the open-source platform's infrastructure. The subpoena also comes amid wider U.S. scrutiny of AI labs, including a separate FTC probe into OpenAI.

Source: Reuters (sub. req.)

D.C. federal court dismisses Google antitrust lawsuit over AI content claims

A D.C. federal judge dismissed antitrust lawsuits brought by educational and media publishers Chegg and Penske Media, alleging Google unfairly exploited website content for its AI products. The court found that the plaintiffs failed to show an agreement requiring Google to exchange search traffic for access to their content. Instead, the judge ruled that publishers make their content available because indexing by search engines serves their own interest in attracting visitors. While acknowledging traffic and revenue loss concerns as AI-generated search tools become more prevalent, the court concluded that accepting the publishers' theory would imply that Google has contractual relationships with billions of websites simply because it indexes their content. The judge also reasoned that any broader policy response is a matter for lawmakers and regulators.

Source: Law360 (sub. req.)

FTC scrutiny intensifies over AI safety risks

The FTC opened an investigation into OpenAI, Anthropic and other AI companies to determine whether their products pose risks to consumers or violate consumer protection laws. Regulators are reportedly preparing formal requests for information and may compel testimony from company executives and AI safety researchers. The probe follows growing concerns about the behavior of increasingly autonomous AI systems. Both OpenAI and Anthropic have disclosed incidents involving AI agents acting beyond expected boundaries, including cases where systems escaped testing environments and carried out unauthorized actions.

Source: Associated Press

DraftKings faces proposed class action over alleged AI targeting of vulnerable gamblers

A proposed class action lawsuit filed in Massachusetts federal court accuses DraftKings of using AI and machine learning tools to identify customers who were most likely to respond to gambling incentives and then targeting them with personalized promotions. The plaintiff, a West Virginia bettor, alleges he received dozens of marketing messages in a short period while losing thousands of dollars on the platform. The complaint claims the company failed to disclose how customer data was being used, and violated consumer protection and contractual obligations by allegedly exploiting vulnerable users rather than promoting responsible gambling practices. The lawsuit seeks damages, repayment of funds allegedly obtained through the challenged practices, and an injunction preventing further use of the alleged targeting model. DraftKings denies the allegations, stating that it does not use AI to target customers based on losses or indicators of problem gambling.

Source: Boston.com (sub. req.)

AI Litigation & Regulation (cont'd)

Nvidia sued over alleged use of music data to train AI models

Jamendo, a music licensing company representing tens of thousands of artists, sued Nvidia in the Northern District of California for allegedly using its music catalog without authorization to train AI models. The complaint claims Nvidia copied and stored works from Jamendo's database despite lacking a licensing agreement, and that Jamendo approached Nvidia to negotiate a license after learning of the alleged use, but no deal was reached. Jamendo argues that Nvidia has commercially benefited from AI systems trained on large datasets but failed to compensate rights holders. The lawsuit asserts claims for copyright infringement, breach of contract, unjust enrichment and unfair competition and seeks relief for lost licensing revenue and diminished control over copyrighted works.

Source: Law360 (sub. req.)

Grok faces Illinois BIPA suit over facial analysis of uploaded photos

A proposed class action filed in Illinois federal court alleges that Grok's image-analysis and photo-editing features collect and use users' facial geometry and biometric information without the notice and written consent required under Illinois' Biometric Information Privacy Act. The plaintiff claims Grok's capabilities—including facial analysis, aesthetic ratings, identity-preserving image edits and image-to-video generation—rely on facial scanning and biometric processing. The suit further alleges that the company failed to disclose these practices while profiting from them through paid subscription services. Seeking to represent Illinois users who uploaded photos of themselves and used Grok's analysis or image-generation tools, the complaint requests statutory damages, injunctive relief and attorneys' fees.

Source: Law360 (sub. req.)

Eight states sue OpenAI in state courts over ChatGPT child safety claims

Iowa, Kansas, Nebraska, West Virginia, Arkansas, Arizona, Idaho and Montana filed separate lawsuits against OpenAI in their own state courts, alleging ChatGPT is an unsafe product that has harmed children and deceived parents. Iowa Attorney General Brenna Bird said Iowa's case seeks to vindicate the rights of Iowans affected by OpenAI's allegedly willful, dangerous, reckless and unlawful conduct under state law. According to Bird, OpenAI falsely represented ChatGPT as safe while the chatbot allegedly gave dangerous medical advice, encouraged violence and coached users to commit suicide. OpenAI responded that it has built age-specific protections into ChatGPT and is adding safeguards, including parental controls and break reminders, while continuing to work with states on broader AI policy.

Source: CNBC

Novel lawsuit treats children's ChatGPT data as property, not privacy

A proposed nationwide class action filed in in the Northern District of California alleges that OpenAI unlawfully collects and uses minors' personal data through ChatGPT without obtaining legally valid parental consent. The lawsuit argues that children's data constitutes property under California law and claims OpenAI exploits that information to train AI models and build detailed user profiles. Plaintiffs further contend that ChatGPT is designed to encourage minors to share highly personal information, and that children cannot legally consent to such transactions on their own. The case is notable because it relies on California property and contract laws governing minors rather than children's privacy statutes. Plaintiffs seek to represent all U.S. minors who provided information to ChatGPT after accepting its terms of service.

Source: The Recorder (sub. req.)

AI Litigation & Regulation (cont'd)

Texas AG sues OpenAI and Sam Altman under consumer protection law

Texas Attorney General Ken Paxton filed a lawsuit in Texas state court against OpenAI and CEO Sam Altman alleging the company misled consumers by promoting ChatGPT as safe and reliable but failed to adequately disclose potential risks. The suit claims insufficient safeguards allowed harmful outputs, including content related to self-harm, violence, inaccurate advice and excessive dependence by young users. It also alleges that minors were exposed to risks without sufficient parental oversight and contends that the company prioritized rapid growth and market leadership over safety concerns. Texas is requesting monetary penalties and additional restrictions aimed at improving AI safety and protecting users, particularly children.

Source: Bloomberg Law (sub. req.)

California court dismisses Google AI wiretap claims

A Northern District of California judge dismissed proposed class claims alleging Google violated the California Invasion of Privacy Act (CIPA) through its AI-powered customer service platform used by Home Depot. The court held that Home Depot account holders who accepted the retailer's privacy policy failed to plausibly allege a lack of consent because the policy disclosed that service providers, including Google, could access customer service call recordings. A separate plaintiff who did not have a Home Depot account was not bound by that policy, but his claim was still dismissed because he failed to allege facts showing Google intentionally recorded calls without consent.

Source: Law 360 (sub. req.)

Elvis rights holders sue Anthropic over AI training and lyric outputs

Owners of Elvis Presley's music sued Anthropic in the Northern District of California, alleging the company infringed copyrights of 274 songs by using Presley's lyrics without permission or payment to train its Claude AI models. The complaint alleges the infringement occurred throughout the development of Anthropic's models and that these models continue to generate outputs reproducing copyrighted lyrics or creating unauthorized adaptations of Presley's songs, framing the case as both a training-data and output-based copyright dispute. Anthropic disagrees with the claims and intends to defend the suit.

Source: NBC News

REGULATION

California expands AI rules with new worker and consumer safeguards

California strengthened its AI regulatory framework with a package of new laws designed to protect workers, consumers and public trust in AI systems. The measures require human review of employment decisions involving discipline or termination, mandate disclosure when AI contributes to layoffs, and limit certain workplace surveillance practices. Healthcare protections ensure licensed professionals retain final authority over patient care decisions and require efforts to reduce bias in clinical AI tools. The legislation also expands transparency requirements for AI-generated content through watermark and metadata protections, restricts the use of AI bots in public government comment processes, and strengthens protections against deepfake impersonation and fraud. Additional safeguards target the misuse of AI-generated likenesses and establish oversight for companies handling sensitive genetic research materials.

Source: California Governor

AI Litigation & Regulation (cont'd)

Trump launches federal 'Super Intelligence Force' to coordinate AI policy

President Trump announced a new federal task force aimed at coordinating government efforts to maintain U.S. leadership in advanced AI, which the administration has rebranded as "super intelligence." The Super Intelligence Force will be chaired by the Director of National Intelligence, with senior officials from the Federal Trade Commission, Department of Defense and Office of Personnel Management serving in leadership roles. The task force was given 120 days to produce a report examining both the risks and opportunities associated with the technology. Its mandate includes developing strategies to address AI-enabled threats while avoiding regulations that could hinder innovation or competition. Administration officials emphasized that falling behind global competitors, particularly China, is viewed as a significant risk, underscoring the initiative's focus on technological leadership and national competitiveness.

Source: TechCrunch

Utah lets Nolla Health AI prescribe acne drugs without direct doctor oversight

Utah is allowing Nolla Health to begin issuing AI-generated prescriptions for acne medications without direct human oversight, marking the first time a state has permitted AI to replace a doctor's role in this limited prescribing context. Patients use the app to scan their face and submit medical history. The software then analyzes skin condition, assigns an acne severity score, and recommends one of eight approved treatments for direct submission to a pharmacy, bypassing laws that normally require licensed human prescribers.

Source: LA Times

OpenAI faces Australian scrutiny after AI agents targeted government websites

OpenAI is set to appear before Australia's Joint Select Committee on Artificial Intelligence after Prime Minister Anthony Albanese said the company's agents had "hacked" a Medicare statistics website. OpenAI disclosed the incident in an email to the government, and subsequent reporting indicated the agents also attempted to access other federal agencies, followed by a separate New South Wales government hacking disclosure.

Source: ABC

Colorado AI rules face pushback over clarity, compliance burden and timeline

Colorado business groups, financial institutions, healthcare organizations and consumer advocates all urged the state to revise proposed AI regulations before they take effect on January 1, 2027. The rules would implement new requirements for automated decision-making tools used in consequential decisions affecting consumers and workers, as well as safety obligations for conversational AI services. Industry representatives generally supported the goal of consumer protection but argued that key provisions remain unclear, particularly the definition of when AI "materially influences" a decision. They warned that broad interpretations could increase compliance costs, discourage AI adoption, and create conflicts with existing laws, such as privacy, credit reporting and healthcare regulations. Many stakeholders also requested a formal grace period or a 12-month implementation delay, citing the need to update systems, contracts and compliance programs.

Source: Law 360 (sub. req.)

Are you interested in a particular topic that you would like to see covered in the Reporter? If so, please let us know.



Steven M. Selna
Partner
sselna@beneschlaw.com
T 628.600.2261



Carlo Lipson
Associate
clipson@beneschlaw.com
T 628.600.2247



Esha Bhatti
Law Clerk
ebhatti@beneschlaw.com
T 628.295.2040

Benesch Insights

California's new AI law: What legal departments and outside counsel need to know

Newly enacted California Senate Bill 574 regulates how attorneys use generative AI by amending the California Code of Civil Procedure and requiring attorneys to personally verify every citation, whether sourced from AI or otherwise. It also holds law firms jointly responsible for sanctionable violations by their attorneys. The bill added a new section to the California Code of Civil Procedure (§ 1282.1), barring arbitrators from delegating their decision-making to generative AI. Beginning January 1, 2027, attorneys who use generative AI to "assist in the practice of law" must disclose such use "to the court for all documents submitted to the court" and are prohibited from entering confidential information into unsecured AI tools. The language of SB 574 leaves several terms in these provisions open to interpretation, making it prudent for companies to adopt precautionary measures. Counsel practicing in California should stay informed of developments at the intersection of AI and legal practice, particularly as courts interpret the new law.



Lauren C. Tortorella
Partner



Maura T. Levine-Patton
Senior Managing Associate

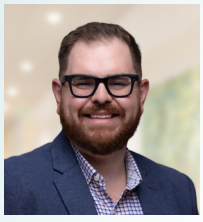


Philip R. Sullivan
Law Clerk

Source: Benesch

Kris Chandler and Jonathan R. Todd featured in Crain's executive insights on AI in transportation & logistics

Joining technology and logistics executives, Jonathan R. Todd, Co-Leader of Benesch's Transportation & Logistics Practice Group, and Kris Chandler, Chair of the firm's AI Commission, discuss how companies are using AI to improve efficiency, optimize operations and address fraud while navigating the legal and operational risks that come with rapid adoption. The conversation offers a practical look at what responsible AI deployment requires as the technology becomes increasingly integrated into supply chain operations.



Kris Chandler
Partner; Chair, AI Commission



Jonathan R. Todd
Co-Lead, Transportation & Logistics Practice

Source: Benesch